PRIVATE BRANCH EXCHANGE (PBX)

PROFILE TEST METHODOLOGY

National Institute for Standards and Technology

DRAFT

Foreword

This publication, Private Branch Exchange (PBX) Profile Test Methodology, is issued by the National Institute of Standards and Technology as part of its program to promulgate security standards for information systems as well as standards for test procedures for assessing the level of conformance, manifested by telecommunications switches, to the said standards. This profile test methodology was developed through the efforts of Dr. Ron Bhattacharyya of Telcordia Technologies (formerly known as Bellcore).

Comments on this document should be directed to:

Dr. Donald G. Marks
NIST/Computer Security Division
100 Bureau Dr., Stop 8930
Gaithersburg, MD. 20899-8930

(301) 975-5342
donald.marks@nist.gov

Table of Contents

1. Introduction

1.1 Identification

- Title: Private Branch Exchange Profile Test Methodology (PBXPTM)
- Registration: National Institute of Standards and Technology
- Keywords: Telecommunications, Switch, PBX, Information Security, Security Assessment, Security Analysis, Testing.

1.2 Overview

The Private Branch Exchange (PBX) is an essential element that supports a "critical infrastructure" of the business community of the country, and protection of the PBX is a high priority. Since the PBX is a Customer Premises Equipment (CPE), the safe and secure upkeep of the PBX and its adjuncts is the responsibility of the customer that owns it. The owner is responsible for paying the telephone bills for calls placed from that PBX, whether the calls are genuine or not. To avoid having to pay for fraudulent calls, it is important that a PBX owner secures the PBX and its adjuncts against unauthorized use and modification/destruction of the embedded process, software and database. NIST has proposed a draft Protection Profile (PP) for the PBX by using Common Criteria.[1] The PP describes a set of standard security requirements that are general enough to be applied to a wide class of PBXs and may be verified through independent testing.

In order to ensure that a PBX conforms to the PP, it is necessary to *test* the PBX to determine its level of compliance. Such testing may be conducted by appropriate "third parties" as long as all testers follow a *uniform test procedure.* This document describes a Profile Test Methodology (PTM), which in essence is a uniform test procedure for assessing the level of conformance of a PBX with respect to the standard security requirements described in the PP. It is recognized that PBXs manufactured by different vendors have different operating systems and the messages they recognize are often vendor-proprietary. As such, to perform an actual test, it will be necessary to carry this PTM to further details that will consist of PBX-specific commands to be executed. *Such details are excluded from this document.* However, the PTM is adequately detailed so that a craftsperson conversant with the command language of a given PBX can use this methodology to perform the test by invoking a complete set of PBX-specific commands and by analyzing the corresponding responses generated by the PBX.

The PTM is intended to be internationally recognized and endorsed by the industry trade associations. It will provide PBX manufacturers and customers with an independent evaluation of security features. The acceptance of these results will improve the security of the entire telecommunications network and allow more open competition among various PBX manufacturers.

[1] *Private Branch Exchange (PBX) Protection Profile* by National Institute of Standards and Technology, March 22, 1999, http://niap.nist.gov/drafts/pbxpp.pdf

1.3 Conventions

This document is organized based on Annex B of Part 1 of the Common Criteria (CC).

Application notes represent guidance and explanations of acceptable implementations for requirements. For additional guidance, the CC itself should be consulted.

1.4 Terms

The following terms, used in this profile, are described in this section to aid in the application of the requirements.

- Adjunct - This is a peripheral device, external to the PBX, but logically connected to it, and supplements the functionality of the PBX by providing additional features. Examples are automated attendant, voice mail system, etc.
- Administrator - An administrator is a user who performs administrative tasks such as creating, retrieving, updating and deleting security parameters (e.g., passwords, permission levels, etc.) in the TOE (Target of Evaluation[2]) database. As such, the administrator has to be a highly privileged user of the TOE. Depending on the organization, the administrator may have titles such as Security Administrator, System Administrator, etc.
- Customer - A customer is a person or organization that is a subscriber to a service offered by a telecommunications service provider. The PBX is a Customer Premises Equipment (CPE).
- Point of Ingress - A point of ingress represents a point of interface with the TOE. Typically, these are ports attached to the PBX console. Two kinds of ports have been invoked in the PTM: (i) the operations port and (ii) the call-traffic port. Operations ports allow access to the PBX to perform operations functions such as provisioning, maintenance, testing, etc. Call-traffic ports allow call-related traffic to be connected to the PBX and its adjuncts.
- Resource - Broadly speaking, there are two types of resources, namely, hardware resources and software resources associated with a TOE. In this PTM, the primary focus is on software resources embedded in the switch. Examples are: the operating system, subsystems, software packages, databases, processes, etc.
- Resource Access - Resources are accessed by transmitting messages to the TOE to impact the software resources of the TOE. Examples include loading a patch, creating, modifying and deleting data, retrieving status reports, initiating a process, etc.
- Subscriber – A subscriber is one who accesses the PBX via its line interface to place and receive telephone calls (and data communication, if relevant). Typically, a subscriber belongs to the organization of the customer that owns the PBX.
- System Access - The system is accessed by establishing an operations session (i.e., login) with the TOE. In order to maintain security of the TOE, system access must be successfully established before resource access is permitted.
- Users - The word “user” is not synonymous with the word “customer” or the word “subscriber.” While a customer is a purchaser of telecommunications service, and a subscriber is the one that places and receives calls (typically, in the customer’s organization), a user is one that is authorized to establish a session at an operations port of the TOE. Typical

[2] See Section 2 for the definition of a TOE.

users of a TOE consist of crafts-persons, administrators, or machines that establish operations related sessions with the TOE. As such, a user could be a person or a machine/system. A valid user must have a user-ID by which the TOE recognizes the user.

- Intruder - An intruder is not authorized to establish a session with the TOE, and as such, is not a user even though the intrusion may be successful.
- Subject – The owner of a process executing on the TOE. Could be a user, customer, or intruder.

2. TOE Description

The PBX Profile Test Methodology (PBXPTM) describes a uniform test procedure for evaluating the level of security that can be associated with a Target of Evaluation (TOE). A TOE consists of the PBX, any adjunct equipment and the software and firmware of the system. A TOE is therefore a *PBX system,* rather than simply a PBX. Those portions of the TOE that must be relied on for the correct enforcement of the TSP are collectively referred to as the TOE Security Functions (TSF). The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement. The security assessment of a TOE is concerned with identifying the security-related features that are available in the TSF as well as the standard security features that are missing from it.

A PBX is essentially a switch that is connected to a telephone company's switch via incoming and outgoing trunks (or lines). These trunks (lines) branch into multiple *extensions* as per that customer's specifications. These extensions are used by subscribers (in the customer’s organization) to place and receive calls. The PBX has embedded software containing specifiable data and translations, which ought to be customized and maintained by the customer (i.e., the PBX owner) to satisfy individual needs. For example, it is possible to specify which extension(s) may or may not receive direct calls from the outside. Similarly, the "Toll Diversion" feature makes it is possible to specify which extension may have what level of permission to place calls, e.g., intercom only, local, long distance, international, etc. These customizations are made by setting appropriate parameters in the PBX software.

Occasionally, two other peripherals are deployed as "adjuncts" to the PBX. One is the "Automated Attendant", and the other is "Voice Mail". An automated attendant is a customer premises equipment which automates the functions of a human receptionist. If an incoming call to an extension of the PBX is not answered, or if that extension is busy, the voice mail system can play a recorded message to the caller, and record an incoming message that the caller wishes to leave.

A PBX has two kinds of ports: call-traffic ports and operations ports. The call-traffic ports support the communications traffic. In other words, wires, cables, trunks, etc., that are connected to these ports carry the communications traffic. The operations ports allow ingress into the embedded software of the PBX. Crafts-persons and administrators access the operations ports to perform operations functions such as provisioning, maintenance, testing, etc.

Crafts-persons authorized to perform operations on the PBX may belong to different categories depending on the operations functions performed by them and their level of expertise. This function is filled by the use of different *roles*, as specified in the Common Criteria. Different roles need to have different levels of access to the PBX. For example, the maintenance crew does not need access to provisioning commands. In addition, within the maintenance crew a less experienced crafts-person may have only the “read” permission, while an experienced one may be trusted with writing as well as reading. It is even possible for a single person to be authorized different roles. For example, a person who is normally a system administrator may also be authorized to act in the role of a maintenance person on occasion. Supervisors may be authorized to act in any of the roles filled by people they supervise.

In order to protect PBX resources and maintain the quality of service, it is necessary to protect the operations ports from unauthorized use. In addition, the call-traffic ports need to be protected against commission of fraud.

The TSPTM describes a uniform procedure to test whether the TSF *offers* adequate security features, which, *if properly activated*, can protect the call-traffic ports from fraudulent use and the operations ports from unauthorized use. If care is *not* taken to activate the available features, the TOE of course will be vulnerable to fraud and other kinds of security compromise. But the task of confirming whether an available security feature is activated or not belongs to a *security audit*, not to *profile testing*, and hence is excluded from the PBXPTM.

3. Security Environment

3.1 Threats

Threats relate to the chance of a security breech that may lead to events such as disclosure of confidential information, commission of fraud, or service deterioration due to misuse, modification or destruction of physical and/or Information Technology (IT) resources. Thus the threats that a PBX may be subjected to have several dimensionalities. Threats might be caused by outsiders (e.g., intruders) or by insiders (e.g., employees of the service provider). Insider threats are not always a reflection of malice on the part of the employee as they may also be the result of inadvertent employee actions. In order to mitigate these threats, one needs to protect the PBX by implementing appropriate security measures.

Examples of threats are listed below.

- Physical threat - Physical damage to a PBX may be caused by natural causes such as fire, flood, earthquake, or by human action such as sabotage. This PTM assumes that PBXs are installed in a physically secure environment. Hence physical security is not addressed here as an issue.
- Fraud - In the context of telecommunications, fraud implies successfully completing a call (voice or data) without paying the legitimate bill for the call. This can be done in several ways if proper precautions are not taken. Examples of fraud include:
- DISA Misuse - A PBX may be equipped with a feature called the Direct Inward System Access (DISA)[3] which allows a subscriber to call the PBX from outside the PBX system, and then obtain a dial tone to place a call to a directory number outside the system. This feature allows a subscriber (such as, a traveling employee of a company) to call the company PBX from outside (i.e., via the trunk interface), and then use the company's telephone service to place calls, which may be economical compared to using a credit card to place long distance calls. However, if this access is not protected, an intruder may place calls at the expense of the PBX owner.
- Misuse of Voice Mail - If the voice mail is configured such that an outside caller is allowed a second dial tone (e.g., by dialing zero after the recorded message is played), an intruder may misuse this facility to place fraudulent calls after receiving the second dial tone.
- Black Box Fraud - Black Box fraud is committed when a Customer Premises Equipment (CPE) is "altered" (i.e., tampered with) in such a way that it becomes possible to place a call to that CPE and successfully complete that call without the caller being billed. Thus, if a fraudulent owner of a PBX deactivates the "Answer Supervision" feature of that PBX, it may be possible to place (and successfully complete) a "free call" to the PBX from a remote location (i.e., no bill is generated for the call). In order for the free call to be successful, it is also necessary that the telecommunications switch at the remote location allow voice transmission[4] in spite of the fact that it (the remote switch) never received the Answer Supervision message from the PBX.

[3] DISA is an optional feature. Hence, in any given application, if DISA is not needed, it may not be deployed.

[4] There are switches that do not allow voice transmission without first receiving the answer supervision message from the called party, thus eliminating the chance of this kind of fraud. But several major switches do not provide

- Misuse of Attendant - If an Automated Attendant is configured in such a way as to provide a second dial tone without adequate verification of the caller, fraudulent calls can be placed after receiving the second dial tone.
- Cloning Wireless Telephone[5] - This applies in the case of a PBX that allows wireless extensions to its subscribers. A wireless phone has several "identifiers" (i.e., attributes by which one phone can be distinguished from another), out of which two are most commonly used for identification purposes. They are the Mobile Identification Number (MIN) and Electronic Serial Number (ESN). It may be possible for an interloper to find out the MIN and ESN of a legitimate subscriber. For example, the interloper may use a radio receiver to eavesdrop when the legitimate subscriber establishes a call, and pick up the corresponding MIN and ESN. Alternatively, the interloper may break into the database that contains the MINs and ESNs of a number of legitimate subscribers. With the knowledge of the MIN and ESN of a legitimate subscriber, the interloper may program them into a cloned phone and use the cloned phone to place calls. The PBX owner will be billed for these calls.
- Voice Mail Intrusion - If an intruder is able to crack the PIN number of a valid subscriber, the mailbox may be taken over by that intruder. This allows the intruder to perform activities such as listening to messages, and using the mailbox as a bulletin board.
- Illegally assigning free lines - This requires entering the operations database of a PBX and the voice mail to perform illegal provisioning.
- Denial of Service – Attacks exploiting vulnerabilities in the protocols may lead to deterioration or even denial of service or functionality of the PBX. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service.
- Access Misuse – Misuse may occur either from legitimate users (i.e. insiders) or intruders. An authenticated user may perform an incorrect operations function (e.g., by mistake or out of malice) and may cause unauthorized modification, destruction, deletion, or disclosure of the PBX software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.
- Intrusion - An intruder may spoof as a legitimate user and break into an operations port of the PBX. At this point the intruder may misuse the permission level of the legitimate user and perform damaging operations functions such as:
  a) Modifying call restriction features of subscribers (e.g., only local calls, long distance calls, international calls, etc.)
  b) disclosing confidential data
  c) causing service deterioration by modifying the PBX software
  d) crashing the PBX

this protective feature. Besides, for Advanced Intelligent Network (AIN) applications, this protection may not be implementable.

[5] The threat of fraud by cloning has been mitigated by the introduction of new technology such as "RF Fingerprinting", and "Authentication via Secret Key Exchange (e.g., by using the CAVE algorithm)." These allow enhanced validation (beyond MIN and ESN confirmation) of a legitimate customer against an interloper, and disallow fraudulent calls.

  e) removing all traces of intrusion (e.g., modifying the security log) so that it may not be readily detected

- Insecure State Transition - At certain times the PBX may be vulnerable due to the fact that it is not in a secure state. For example:
  - After a system restart, the old security features may have washed out, and new features may not have been activated. (For example, all old passwords have reverted to the default system-password, and new passwords have not been assigned.)
  - The same may happen at the time of a disaster recovery.
  - At the time of installation the PBX may be vulnerable until the time that the default security features are customized.
- Insecure Security System - The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for later intrusions. For this reason, the security system must be carefully protected.

3.2 Organizational Security Policies

The PBXPTM intrinsically assumes the existence of several security-related organizational policies that include the following:

- P.Access - Access rights to specific data objects are determined by object attributes assigned to that object, subject identity, subject attributes, and environmental conditions as defined by the security policy. A service that a subject is not authorized for shall be denied to that subject.
- P.Availability - There shall be no denial of authorized service. A TOE access that a user is authorized for shall not be denied to that user. A service that a subscriber is authorized for shall not be denied to that subscriber.
- P.Resiliency - If a security compromise occurs, the TOE shall continue to provide those services unaffected by that compromise.
- P.TMN Standards - The tasks related to “Prevention”, “Detection”, “Containment”, “Recovery”, and “Security Administration”, as defined under TMN (Telecommunications Management System) standards, shall be recognized and delegated to appropriate authorities. Prevention implies physical security, legal review, risk analysis, and logical controls. Detection is associated with alarms, cameras, usage pattern analysis, revenue pattern analysis, security audit, investigation of security breech, etc. Containment and recovery, as the names imply, include intrusion recovery, disaster recovery, legal action, apprehension, etc. Security administration involves the day to day activities of ensuring that protective features are activated, the security parameters are kept up to date, and the security weaknesses are corrected.
- P.Confidentiality - Confidential information shall not be made available to unauthorized entities (persons, machines, etc.).
- P.Training -Authenticated users of the system shall be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the non-discretionary controls implemented to enforce these policies.
- P.Usage – TOEs shall be used only for authorized purposes.

- P.Traceability - The TSF shall implement features (e.g., alarms, audit trails, etc.) to: (i) alert an administrator of a suspected security breech, and (ii) record security events in a log file so that in case a breech is suspected, an audit trail could be established as part of investigation, and (iii) record adequate audit detail to uniquely identify subjects, ports, and security relevant activities.
- P.Administration - The authorized administrator shall properly activate, implement and maintain the security features of the TSF.
- P.Accountability - Each user in the organization shall be held accountable for TOE-related actions performed by that user.

3.2. Security Usage Assumptions

This section describes the security aspects of the environment surrounding the TOE installation. This includes information about the physical, personnel, and connectivity aspects of the environment.

3.2.1 Physical Assumptions

The PBXPTM does not include any test to assess the *physical security* of the environment. It is assumed that the resources of the TOE, except possibly the remote access facilities, will be installed in a physically secure environment which will be "reasonably safe" from typical natural hazards as well as from unauthorized physical access. An example of a "reasonably safe" system implies the following, as a minimum:

- A.Natural. The TOE shall be protected from environmental hazards.

- A TOE[6] shall be housed in a facility that shall conform to established local building standards, i.e., codes related to precautions against hazards due to fire, flood, earthquake, and inclement weather conditions such as tornado, hurricane, typhoon, etc. This includes, among other construction codes, appropriate installation of various types of alarms and an administrative mechanism to promptly respond to such alarms when activated.

- A.NoBreakIns. The TOE shall be adequately protected from intruders obtaining physical access to the TOE or related equipment, by means such as:
  - Lighting within and around a facility shall provide adequate visibility for security guards and cameras.
  - Entry into a facility from outside shall be restricted by means of electronic locks or trained guards & ID cards.
  - All doors for entering the premises shall be alarmed during hours that are outside the normal business hours. All "exit only" doors (especially emergency exits) shall be alarmed all the time.

[6] If the TOE includes ubiquitous Network Elements such as broadband switches and routers, it may not always be feasible to guarantee a physically secure environment for them.

  - All facility access points, parking lots or other designated areas shall be equipped with 24-hour camera monitoring.
  - Terminals used for local access shall have the same level of physical security as that of the TOE.

- A.PhysicalAuthorization. Physical access to the TOE shall be controlled and restricted to those needing such access, through such means as:
  - All persons (i.e., employees, contractors, authorized visitors, etc.) in a TOE facility shall be issued appropriate company-designated badges that authorize the holders to specific facilities or areas which they need to access.
  - Within a given TOE facility, areas which are considered critical/sensitive shall have doors protected with electronic locks that allow entry only to authorized personnel, based on need to access. These doors shall be spring-loaded so that they will automatically close after they have been opened.
  - All visitors to a TOE facility shall sign and date a visitor log, shall be issued a visitor badge and, if necessary, be escorted. The log shall, as a minimum, record the visitor's name, the name of the establishment he/she represents, citizenship, the TOE point of contact, purpose of visit, date and times of arrival and departure.
  - All visitor badges shall be date and time limited.

3.2.2 Connectivity Assumptions

It is assumed that the following connectivity assumptions exist:

- A.Ingress. It is assumed that there are three types of ingress into the operations ports of a TOE, namely, local access, remote dial-up access, and remote networked access.
- Operations Systems (OS), in general, shall access the TOE from remote locations, either via dial-up access or via networked access.
- There may be human users who are authorized to access the TOE from terminals situated at remote locations, and they may use dial-up access or networked access directly to the TOE.
- A.Protocols. Networked accesses may use a wide range of protocols such as X.25, TCP/IP, CMIP, SNMP, SS7 (for Common Channel Signaling), and several proprietary protocols.
- A.InsecureRemote. Remote locations shall not be assumed to be secure.
- A.InsecureNetwork. Depending on the network connectivity, the network may or may not be secure.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. The uniform test procedure described in the PBXPTM is geared towards assessing whether the TOE meets these security objectives.

4.1 IT Security Objectives

- **O.KNOWN**: The TOE shall ensure that, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access to the TOE or its resources.
- **O.ACCESS**: The TOE shall allow access by authenticated users to those TOE resources for which they have been authorized, and deny access to those TOE resources for which they are not authorized.
- **O.AUTHORIZE**: The TOE shall provide the ability to specify and manage "resource access permission" to be assigned to its users.
- **O.BYPASS**: The TOE shall prevent all software and users from bypassing or circumventing TOE security policy enforcement.
- **O.ACCESS-MALICIOUS**: The Toe shall mitigate the threat of malicious actions by authenticated users (e.g. by holding an authenticated user accountable).
- **O.ACCOUNT**: The TOE shall ensure that all TOE users can be held accountable for their security-relevant actions.
- **O.INFO-FLOW**: The TOE shall ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.
- **O.OBSERVE**: The TOE shall ensure that its security status is not misrepresented to the administrator or user.
- **O.DETECT**: The TOE shall have the capability to detect system failure and breech of security.
- **O.RECOVER**: The TOE shall provide for recovery to a secure state following a system failure, discontinuity of service, or detection of a security flaw or breech.
- **O.AVAILABLE**: The TOE shall protect itself from denial-of-service attacks, including those due to shared resource exhaustion.
- **O.NETWORK**: The TOE shall have the capability to meet its security objectives in a networked environment.
- **O.CONFIDENTIAL**: The TOE shall have the ability to identify confidential information. Such information may be related to customers, or system security. The TOE shall release confidential information only to authorized users.

4.2 General Assurance

It is desirable that applications, which require several distributed PBX installations interconnected with one another, shall provide layered security administration, in compliance with TMN standards. These standards specify five layers defined as:

- Business Management Layer (BML) - which will be responsible for tasks such as Security policy, Disaster recovery plan, Assessment of data integrity, etc.

- Service Management Layer (SML) - which will perform functions such as Administration of certification, Administration of security protocols, Customer audit trail management, and Customer security alarm management.
- Network Management Layer (NML) - which will perform administration of security parameters at the overall network level.
- Element Management Layer (EML) - which will perform administration of security parameters of a group of similar PBXs.
- Network Element Layer (NEL) - which will provide local access at the PBX console.

It follows from the above definitions, that while BML and SML take care of the business and service related concerns associated with security, the three lower layers, namely, NML, EML, and NEL perform the PBX operations in a hierarchical way. Hence it is assumed that, as a minimum, these three layers will provide the required connectivity for distributed PBX operations.

5. Profile Test Methodology

This chapter describes the Profile Test Methodology, which, in essence is a uniform test procedure that can be applied to the TSF described earlier for assessing the security of the corresponding TOE. The tests are nondestructive, and they are independent of the traffic load of the TOE. As such the tests do not require the deployment of any specific load boxes.

5.1 Points of Ingress

The first step in the test procedure is to identify *all* points of ingress into the TOE. A PBX offers two kinds of ingress: call-traffic ingress and operations ingress. Call-traffic ingresses allow call-related traffic to be connected to the TOE, which includes the PBX and its adjuncts. Operations ports allow access to the TOE to perform operations functions such as provisioning, maintenance, testing, etc. All of them must be included in the scope of the PTM.

5.1.1 Call-Traffic Ingress

Call-traffic ingresses do not allow unauthorized access into the embedded resources of the TOE. However, if not adequately protected, these ingresses can be accessed to commit fraud. The ingresses that are especially susceptible to the commission of fraud are the DISADN (Direct Inward System Access Directory Number), voice mailboxes of the PBX subscribers, and the DN corresponding to the automated attendant. Consequently, the PBXPTM must include tests to determine whether such ingresses are adequately protected against fraud.

5.1.2 Operations Ingress

Operations ingress, in general, belong to three categories:

> **Local Access:** A workstation at the console of the TOE provides local access. If the TOE is installed in a physically secure environment, it can be expected that the workstation and its connectivity to the TOE are also physically secure. The implication is that the workstation is out of reach for a subject who is not authorized for physical access to the TOE. Further, the connecting cables constitute a “trusted path”, i.e., an outsider cannot tamper with them. Thus, to secure a local access, it has to be ensured that all users who are authorized for physical access to the TOE are held accountable for their actions.
>
> **Dial-UP Access:** If a modem is connected to a port at the operations console of a TOE, it may be possible for a subject to dial up the modem from a remote location and establish an operations session with the TOE via the modem. A dial-up access, in general, is more vulnerable to spoofing than a local access. Hence security requirements are more stringent for a dial-up access, which, in turn, require more elaborate testing.
>
> **Network Access:** If a port of the TOE constitutes a node of a network (e.g., Corporate Network, Internet, X.25, etc.), it may be possible to access the TOE from other nodes via the network. Consequently, the PBXPTM must include tests to determine whether such ingresses are adequately protected against unauthorized access.

Thus, the first task is to identify all the points of ingress into the TOE, and group them into the categories listed above.

5.2 Tests for the Call-Traffic Ingress

5.2.1 Protection of DISA

1. Establish a login as an administrator at an operations port, and retrieve the table corresponding to the DISA feature. Verify if the DISA feature is optional (i.e., a customer is *not* offered the DISA feature unless the customer specifically asks for it). If the DISA is a hardcoded feature that cannot be deactivated, the TOE fails the test.
2. Activate the DISA feature, and attempt to assign a DN (which is less than ten digits in length) for the DISA application. If the transaction is executed, the TOE fails the test.[7]
3. Assign a ten-digit DISADN. Verify that the assignment is executed (otherwise the TOE fails the test). If executed, check whether the DISADN has an assignable aging feature. If there is no assignable aging feature, the TOE fails the test.
4. If the DISADN offers an assignable aging feature, assign 30 days as the aging interval for the DISADN. Advance the clock beyond the aging interval (i.e., more than 30 days). Dial the DISADN. If the call is accepted (i.e., if the DISADN has not expired in 30 days), the TOE fails the test.
5. Establish a login as an administrator at an operations port and attempt to assign a PIN number (which is less than ten digits in length) for a DISA access. If this transaction is executed, the TOE fails the test.[8]
6. Assign a ten-digit DISA-PIN number to a subscriber. Verify that the assignment is executed (otherwise the TOE fails the test). If executed, dial the DISADN as the subscriber and perform the following tests:
    - Check if there is a second dial tone before the PIN is provided. If there is one, the TOE fails the test.
    - Instead of providing the PIN, dial several typical numbers such as 0, *, #, 9, 00, 99, 011, 411, 911, etc. If any of these attempts generates a second dial tone, the TOE fails the test.
    - Dial five incorrect PINs in succession and check if a second dial tone can be obtained. If there is one, the TOE fails the test.
    - Check whether an alarm is generated as a result of dialing the incorrect PINs. In addition, check whether the event is recorded in a security log. Both checks should be positive. Otherwise, the TOE fails the test.
    - Provide the correct PIN and check if there is a second dial tone. If not, the TOE fails the test.
7. Establish a login as an administrator at an operations port and retrieve the file that has stored the PIN. If the PIN can be retrieved in plaintext, the TOE fails the test.
8. From the attributes associated with the DISA-PIN, check whether the PIN can be assigned an aging feature. If there is no assignable aging feature for the PIN, the TOE fails the test.
9. If the PIN has an assignable aging feature, assign 30 days as the aging interval for the PIN. Advance the clock beyond the aging interval (i.e., more than 30 days). Dial the DISADN as the subscriber and verify whether the PIN has expired. If not, the TOE fails the test.

[7] A DISADN must be at least 10 digits in length.

[8] A DISA-PIN must be at least 10 digits in length.

10. Establish a login as an administrator at an operations port. Create four different *authorization codes* for four subscribers respectively, where the four authorizations are for “Intercom only”, “Intercom plus local calls only”, “ All calls except international calls”, and “All calls including international calls”. If the authorization codes do not offer this granularity, the TOE fails the test.
11. Dial the DISADN and provide the DISA-PIN for a subscriber who is authorized for “Intercom only.” After receiving the dial tone, dial an outside number (not an intercom extension). If the call is successfully places, the TOE fails the test.
12. Repeat Step 11 for the other three subscribers and check if the authorization code is effective each time. If not, the TOE fails the test.

5.2.2 Protection of Adjuncts

1. Establish a login at an operations port of the voice mail system and retrieve the attributes of PINs associated with mailboxes. Check if the attributes include the following:
   - A string of less than seven digits cannot constitute a valid PIN for a mailbox.
   - A PIN, which is the same as the phone number associated with a mailbox, cannot be a valid PIN for that mailbox.
   - A PIN has an aging feature
   - A PIN is changeable by the corresponding subscriber

   If any of the four conditions is not satisfied, the voice mail system fails the test.
2. As an administrator, assign a mailbox with a PIN to a subscriber’s extension. Initiate the “off-hook” condition (i.e., pick up the phone) as that subscriber, and attempt the following:
   - Change the PIN to a string of less than seven digits.
   - Change the PIN to the same extension number (and/or phone number) of the subscriber.

   Unless both transactions are denied, the voice mail system fails the test. Next, change the PIN to a valid string of acceptable length (seven digits or more, depending on the system configuration). If this transaction is denied, the voice mail system fails the test.
3. From another DN (or extension), dial the subscriber’s extension. Ensure that the subscriber does not pick up the phone, so that the voice message is played. At this point, dial several typical numbers such as 0, *, #, 9, 00, 99, 011, 411, 911, etc. If any of these attempts generates a second dial tone, the TOE fails the test.
4. From a DN outside the PBX, dial into the voice mail system and attempt to break into the mailbox of a subscriber by repeatedly guessing the PIN. Within five consecutive cracking attempts, if the mailbox does not get locked against further attempts, the voice mail system fails the test.
5. Establish a login as an administrator of the voice mail system, and perform the following tests:
   - Check whether an alarm has been generated due to the PIN-cracking attempt described above. If there is no such alarm, the voice mail system fails the test.
   - Retrieve the security log. If the PIN-cracking attempt described above is not recorded in the security log, the voice mail system fails the test.
6. Establish a login as an administrator of the voice mail system and attempt to retrieve the list of mailboxes that are unassigned. If the administrator does not have this capability, the voice mail system fails the test.
7. From a DN outside the PBX, dial into the automated attendant (if there is one), and listen to the voice menu as to whether it reveals how to get a dial tone. If the message reveals this in-

formation, the automated attendant fails the test. If there is no such information is conveyed in the message, dial several typical numbers such as 0, *, #, 9, 00, 99, 011, 411, 911, etc. If any of these attempts generates a second dial tone, the automated attendant fails the test.

5.3 Tests for the Operations Ingress

Typically, all the components of the TOE, such as the PBX, the voice mail system, and the automated attendant have their respective operations ingresses. These ingresses are used by craftspersons and administrators to Create, Retrieve, Update, and/or Delete (CRUD functions) the software, translations, and databases of the corresponding components. Hence these ingresses need to be protected from unauthorized use by an "outsider" (e.g., an intruder) or by an "insider" (e.g., a disgruntled employee). Since the security issues are approximately the same for all the components, the tests are presented here in a generic way, and the word TOE implies a totality of all the components. All the operations ingresses into the TOE need to be tested as described in the following sections.

5.3.1 User Identification

Identification is the process of recognizing a user'*s* unambiguous and auditable identity with the help of an *identifier* that is typically referred to as the user-ID. In general, the user-ID need not be confidential. It is the unambiguous name of a *user* by which the user can be held accountable. As such, all actions initiated by a user need to be associated with the corresponding user-ID. The corresponding PTM includes the following steps:

1. At a point of ingress typically used by the administrator (also called superuser), establish a login as the administrator. Print out the list of all user-IDs and other user attributes (such as role, privilege, etc., which are not confidential). Check if there is any recurrence of user-IDs, i.e., multiple users with the same user-ID but different in other user attributes. If a recurrence is observed, the TOE fails the test.
2. Enter the command to create a new user-ID that already exists, and check whether the TOE denies this transaction. If the TOE does not deny this transaction, it fails the test.
3. Create a new user-ID (i.e., one that did not exist before). Advance the TOE clock by three months. Check if the user-ID is disabled. If the user-ID is not disabled, the TOE fails the test.
4. The test for verifying the association between a user-ID and actions initiated by that user-ID is described under "Security Log" in Section 5.6.

5.3.2 User Authentication

Authentication is the process of verifying the claimed identity of a user. Depending on the TOE, there could be different kinds of authenticators such as passwords, tokens, smart cards, key-based authenticators, voice recognition, retina scan, etc. No matter what type of authenticator is used, it is of critical importance to ensure that the authenticator of one user cannot be spoofed by another. The corresponding PTM includes the following steps:

1. Login as the administrator. If the authenticator is a password, enter the "retrieve" command to retrieve the password file on the screen, and the print command to print the file. (These commands must not result in retrieving or printing passwords in *plaintext*.) The TOE is al-

lowed to either deny these transactions, or retrieve/print passwords in cyphertext. If the transactions are denied, the TOE passes this test. However, if *cyphertext* passwords are available to the administrator, check if this privilege (i.e., access to cyphertext passwords) can be denied to all other users. If not, the TOE fails the test. If yes, then confirm this feature by logging on as a user who is *not* an administrator, and repeat the retrieve and print commands for the password file. The TOE should deny these transactions. If not, the TOE fails the test. (Note: plaintext passwords must not be available to any user including the administrator. Cyphertext passwords may be available to the administrator, but not to any other user).

2. In Step 1, while logging in, check if the password is echoed in plaintext. If the echo occurs, the TOE fails the test.
3. Login as the administrator, and create a new user-ID and the corresponding password. Log-off, and then login as the new user. At this point, the TOE must ask the new user to change the password. If not, the TOE fails the test.
4. If the TOE passes Step 3, change the password to a common English word or name. If the TOE accepts this new password, it fails the test. If the TOE rejects the common English word or name, try longer English words (i.e., six or more letters). The TOE should reject all these words also. Otherwise it fails the test. If the TOE rejects all the English words attempted so far, try a combination of alpha and numeric characters with a string-length of less than six characters. If the alphanumeric string of less than six characters is accepted as a password, the TOE fails the test. Continue increasing the length of the alphanumeric string one character at a time, up to sixteen characters if needed. On or before the alphanumeric string reaches a length of sixteen characters, the TOE should accept the new password (if not, the TOE fails the test).
5. Subsequent to Step 4, i.e., when the newly assigned password has been updated by the user, advance the clock of the TOE by 60 days, and try to login using the same password. The TOE should deny the login. If the denial occurs, the TOE passes the test. If the denial does not occur, look for an admin command to assign the password-aging interval. If there is no feature for assigning the aging interval, the TOE fails the test.
6. If the TOE offers the feature for assigning the password-aging interval, check whether the assignment can be individualized on a user-ID basis or on a port basis. If not (i.e., if the assignment is on a system-wide basis), the TOE fails the test.[9]
7. If the TOE passes Step 5, i.e., if after advancing the clock by 60 days the password expires, update the expired password without changing it (i.e., the new password is the same as the old). The TOE should deny this transaction. If not, the TOE fails the test.
8. If the TOE passes Step 7, update the old password with a new password (from P1 to P2). Advance the clock again by 60 days, at which point P2 expires. Now try to change it to P1 back again. The TOE should deny this transaction. Otherwise, it fails the test.
9. Login as an administrator and create two user-IDs and assign the same password to both of them. The TOE *should allow* this transaction. Otherwise it fails the test.
10. If the TOE passes Step 9, login separately as the two users created in Step 8. When the TOE asks for the passwords to be changed (see Step 3), update the passwords such that both have

[9] For machines, such as Operations Systems, that stay logged on to the TOE on a long-term basis, there should be aging of the password of that machine. For a remote OS, which is continuously logged on to a TOE, if the session gets interrupted due to reasons such as power failure, an expired password may be a hindrance to re-establishing the session, especially if the OS is rarely attended by human users.

the same updated password. The TOE *should allow* this transaction.[10] Otherwise, the TOE fails the test.

11. For each point of ingress that allows a network access, establish several consecutive sessions (i.e., logins) and verify that a one-time authentication mechanism is in place, i.e., each time the authenticator is different.[11] If not, the TOE fails this test.
12. Repeat Step 11 for each point of ingress that allows a dial-up access. If the access requires one-time authenticators (as described above), the TOE passes the test. If not, check if the dial-up access is compatible with a smart modem with secure dial-back capability. If not, the TOE fails the test.
13. Establish a login as an administrator. Create two user-IDs and assign passwords to them. Initialize the TOE (i.e., system restart) and check if the same passwords are maintained. If not (e.g., if the passwords revert to a default password), the TOE fails the test.

5.3.3 System Access Control

System Access Control authorizes establishment of a session (i.e., login) and continuation of a session until logoff. There are certain restrictions regarding the login procedure, i.e., how a session is established and how it is sustained. The corresponding PTM includes the following steps:

1. Establish a login at each ingress point. Each ingress (except for the EAI[12]) should require the user to provide a user-ID and an authenticator (such as a password, a one-time authenticator, etc.). If this requirement is not fulfilled, the TOE fails the test.
2. At each ingress (except for the EAI), check if a warning banner is displayed at the time of the login. If there is no warning banner, the TOE fails the test.
3. At each ingress (except for the EAI), attempt to login with an incorrect user-ID. Repeat the login attempt with a correct user-ID but incorrect authenticator. Check whether the TOE responds with a helpful message (e.g., the user-ID is incorrect, or the password is incorrect).[13] If there is a helpful message, the TOE fails the test.
4. At each ingress (except the EAI), continue the login attempt with incorrect user-ID/authenticator combination. On or before the fifth consecutive attempt, check whether the TOE raises an alarm and locks the channel for a limited time (not more than ten minutes). If not, the TOE fails the test.
5. At each ingress (except the EAI), establish a successful login and check whether there is a display of the date and time of the last successful login and the number of unsuccessful attempts made since the last login. If not, the TOE fails the test.
6. At each ingress (except the EAI), establish a successful login and advance the clock by 30 minutes. If the session is not timed out, the TOE fails the test. Also, test whether the session could be re-initiated by providing the authenticator. If not, the TOE fails the test.
7. At each ingress (except the EAI), establish a successful login. Next, disconnect the cable connecting the workstation to the TOE. Connect it back again, and check if a login is needed

[10] If two users, unbeknownst to each other, happen to choose the same password, the TOE should not deny it, because a denial reveals the existence of a password.

[11] Examples of “one-time authenticators” are Secur-ID, Kerberos, encrypted strings containing time stamps, etc.

[12] A TOE may be equipped with an Emergency Access Interface (EAI) which allows a session without a login so that in the case of an emergency, when the regular login feature does not function, the TOE, as a minimum, can be restored via the EAI.

[13] The acceptable response is that the login attempt is invalid, without any suggestion as to the cause of the failure.

to establish a session. If a login is not needed (i.e., if the previous session did not terminate as a result of the cable disconnection), the TOE fails the test.

8. At each ingress (except the EAI), establish a successful login. Next, turn off the power for the workstation. Turn the power back on again, and check if a login is needed to establish a session. If a login is not needed (i.e., if the previous session did not terminate as a result of the "power off"), the TOE fails the test.
9. At each terminal check for the mechanism to lock the keyboard. If there is no such mechanism, the TOE fails the test. If the mechanism is available, continue the test and check if the time-out feature is suspended during the interval that the keyboard remains locked. If the time-out feature is *not* suspended, the TOE fails the test.
10. If the TOE passes Step 9, test whether a locked keyboard can be unlocked by providing the authenticator. If not, the TOE fails the test.
11. If the TOE is equipped with an EAI, establish a session at the EAI, and check the following:
    - The TOE should raise an alarm indicating that the EAI has been accessed.
    - Enter a command to restore the TOE from its disk image, and the TOE should perform the transaction.
    - Enter a command that is not related to TOE restoration (e.g., issue a command to create new user-IDs and passwords), and the TOE should deny this transaction.

    Unless the three conditions are met, the TOE fails this test.
12. If the TOE consists of numerous small distributed switches and routers (as may be case for emerging PBXs), which are administered from a centralized Element Management Layer (EML) or a Network Management Layer (NML), perform the following tests:
    - Establish a login at one of the switches and enter a command such as "OPEN <IP ADDRESS of another switch>." If, as a result, access is established, without authentication, to the other switch at the IP Address specified in the command, the TOE fails the test.
    - Enter a command from the centralized environment (e.g., the EML) to lock the local access to all the switches constituting the TOE, so that a login at the switch console will be denied. Verify the result by attempting to establish local sessions at several switch consoles. The switches should deny these login attempts. Otherwise, the TOE fails the test.
    - If the switches, as default, accept SNMP (Simple Network Management Protocol) messages without a login, enter a command from the centralized environment (e.g., the EML) to disable the SNMP compliance. Now transmit several SNMP messages, and the switches should reject the SNMP messages. Otherwise the TOE fails the test.
    - If the switches, as default, accept other protocols such as SPANS (Simple Protocol ATM Network Signaling), UNI (User to Network Interface), etc., without requiring a login, repeat the above bullet-listed test for each such protocol. If the mechanism of accepting messages without authentication cannot be disabled, the TOE fails the test.
    - If the TOE includes SONET (Synchronous Optical Network) rings connecting several ADMs (Add Drop Multiplexers), such that access from one ADM to another may be possible over the DCC (Direct Communications Channel), establish a login at the *Crafts Interface* (not the *Admin Interface*)[14] of an ADM. Transmit the "SELECT <NE>" command to access another ADM. If, as a result, access is established, without authentication, to the other ADM that has been specified in the command, the TOE fails the test.

[14] The Admin Interface may be designed to access other ADMs on the SONET ring.

13. For operations-related ingresses to the TOE that are required to be compliant with the TMN standards, perform the following tests:
    - Test whether CMIP (Common Management Information Protocol) is used for security management messages transported to the ingress from a corresponding OS (Operations System) and test whether SSL3 (Socket Layer, Version 3) is used for messages transported over TCP/IP. If neither protocol is in use, the OS/TOE interface is not TMN-compliant.
    - For the case of CMIP, check if it uses STASE-ROSE (Security Transformations Application Service Element for Remote Operations Service Element) by performing the following tests:
        a) Check whether the ROSE PDU (Remote Operations Service Element Protocol Data Unit) is protected by applying selected ST (Security Transformation) to the whole PDU encoded with a symmetric key in conformance with DER (Distinguished Encoding Rules).
        b) Check whether STASE-ROSE computes a hash-based MAC (Message Authentication Code) of the DER-encoded ROSE PDU as well as a secret password, and appends the result to the ROSE PDU for integrity protection.
        c) Check whether STASE-ROSE computes the MAC of the DER-encoded ROSE PDU and appends the result to the *encrypted* ROSE PDU for integrity and privacy protection.

        If the above checks yield negative results, the TOE ingresses that are supposed to be TNM-compliant by using the CMIP interface fail the test.
    - For the case of SSL3 over TCP/IP, test whether the following conditions hold:
        a) Strong peer entity authentication, based on public key encryption, is used for all associations
        b) A public key certificate from the TMN's CA (Certification Authority) is available
        c) Session secret is encrypted with receiver's public key
        d) SHA1 (Secure Hashing Algorithm 1) is used by SSL3 for integrity
        e) For transactions that require privacy, DES (Data Encryption Standard) in the CBC (Cipher Block Chaining) mode is used for symmetric key encryption
        f) Entity public key size is at least 768 bits
        g) CA's public key size is at least 1024 bits
        h) Certificates are X.509, Version 3
        i) Integrity and non-repudiation are computed on plaintext messages
        j) Ciphersuites ESA, NULL, and SHA1 are supported for applications that do not require privacy
        k) Ciphersuites RSA, DES-CBC, and SHA1 are supported for applications that require privacy

        If the above conditions do not hold, the TOE ingresses that are supposed to be TNM-compliant by using the SSL3 interface fail the test.
14. For operations-related ingresses to the TOE that allow network access over the Internet (using TCP/IP), verify whether the following functions/services can be disabled for the TOE (this needs to be done in addition to Step 11 under "User Authentication" in Section 5.3.2):
    - Several services based on UDP (User Datagram Protocol) such as chargen, echo, and discard

- Boot services
- Services based on RPC (Remote Procedure Call)
- r-commands such as rsh, .rhost, etc.
- finger
- RIP (Router Information Protocol) daemon (routed)
- TFTP (Trivial File Transfer Protocol)
- NFS (Network File System)
- NIS (Network Information Services)
- Source Routing
- ICMP (Internet Control Message Protocol) Redirect

If any function/service from the above bullet list cannot be disabled for the TOE, the TOE fails the test.

15. For operations-related ingresses to the TOE that allow network access over the Internet (using TCP/IP), print the "Access List" at each such TOE ingress, and verify whether packets can be rejected on the basis of:
    - Sender's user-ID
    - Sender's password (encrypted)
    - IP addresses of the source and destination
    - Port numbers associated with source and destination
    - Date and time of message transmittal
    - Protocol used
    - Corrupted or fragmented message

    In absence of any of the above restrictions, the TOE fails the test.
16. For operations-related ingresses to the TOE that allow dial-up access, print the database associated with the dial-back mechanism and verify the following (this needs to be done in addition to Step 12 under "User Authentication" in Section 5.3.2):
    - For each user-ID authorized for a dial-up access there should be the authorized directory number for call origination.
    - Subsequent to receiving a login request, the TOE should disconnect the call and originate a new call to the authorized directory number corresponding to the user-ID.
    - For each authorized user-ID there should be a confidential password stored in a one-way encrypted form.

    If the data printout does not support the three bullet items, the TOE fails the test.
17. If the TOE passes Step 17, deactivate the dial-back mechanism (e.g., by switching off the power to the modem). Activate it back again and check if the passwords associated with the authorized user-IDs have reverted to a default password. If this has occurred, the TOE fails the test.

5.3.4 Resource Access Control

Resource Access Control is the capability of a TOE to deny access to a resource of the TOE unless there is proper authorization (e.g., user privilege, channel privilege, terminal privilege, etc.). The corresponding PTM includes the following steps:

1. Retrieve/Print the database containing user-attributes, and check whether a code is assigned to each user-ID that specifies the level of privilege (i.e., authorization level) associated with that user-ID. If no such privilege can be assigned to a user-ID, the TOE fails the test.
2. Retrieve/print the database containing the operations-related commands and check whether for any given command a privilege can be assigned to specify the authority levels required of the user-ID to execute that command. If there is any operations-related command to which any specified privilege cannot be assigned, the TOE fails the test.
3. Establish a login as an administrator. Arbitrarily select a command <C>, and assign a privilege code <P> to that command. Create two user-IDs <U_1> and <U_2>, assign to them privileges <P> and <Q> respectively. Check whether the execution of command C is allowed only when U_1 and denied to $U_{2.}$ If not, the TOE fails the test.
4. Establish a login as a user whose privilege is lower than that of an administrator. Try to execute the command that enhances the privilege of the user to that of an administrator. If TOE executes this command, i.e., if the user is able to elevate his/her privilege to that of the administrator, the TOE fails the test.

5.3.5 Security Log

A Security Log provides tools to establish an audit trail, so that if security breech is suspected, investigation can be made as to whether/how the breech occurred. The corresponding PTM includes the following steps:

1. Establish a login as an administrator and execute the commands for retrieving/printing the history files. If the TOE does not maintain any history file, it fails the test. In addition, if the administrator cannot retrieve and print the history files, the TOE fails the test.
2. Establish a login as an administrator and test whether the history files can be retrieved on a selective basis (e.g., dates/times of beginning and end, events associated with a giver user-ID, and events associated with a given point of ingress). If the administrator cannot select the portion of the history file to be retrieved, the TOE fails the test.
3. If the TOE passes Step 1, perform the following activities:
   a) Create a user-ID, assign a password and a low level privilege code (i.e., a privilege which is lower than that of the administrator) to it.
   b) Attempt to establish a login as the newly created user-ID and an incorrect password, and verify that the TOE denies the request. If the request is not denied, the TOE fails the test.
   c) Establish a login as the newly created user-ID (with the correct password), and attempt to execute the following commands:
      - a command to modify a record in the history file
      - a command to modify a user's security profile (e.g., user-ID, password, and privilege)
      - a command to modify the security profile of a point of ingress (e.g., privilege associated with the ingress)
      - a command to modify the permission level associated with an access (i.e., the authority level needed for the access)
      - a command to modify a system software

   The TOE should deny the attempted transactions. If not, the TOE fails the test.

4. If the TOE passes Step 2, establish a login as an administrator, and retrieve the history files to check if they contain the following records:
   - The Logins that occurred in Steps 1 and 2c
   - The unsuccessful login attempt that occurred in Step 2b
   - The denial of all transactions attempted in Step 2c

   If any of these records are missing from the history files, the TOE fails the test.
5. If the TOE passes Step 3, test whether, the records contain the following attributes for the events recorded:
   - Date and time of the event (including attempted events)
   - The user-ID associated with the event
   - Names of resources accessed
   - Success or failure of the attempt

   If these attributes are missing from the records, the TOE fails the test.
6. Check if any record contains the password (or other authenticator information) of the user associated with the event recorded. If a password in plaintext or cyphertext is recorded in any history file, the TOE fails the test.
7. Retrieve the list of alarms from the database and test if TOE generates an alarm when the history files malfunction. If there is no provision for such an alarm, the TOE fails the test.
8. Initialize the TOE (i.e., system restart) and test whether the history files retain the records. If not (i.e., if the records do not survive a system restart), the TOE fails the test.

5.3.6 Security Administration

This feature entails proper activation, maintenance, and usage of the security features of a switch, conducted by an appropriate administrator. It includes overriding vendor-supplied defaults, keeping the security parameters up to date, monitoring suspected activities, and generating security audits when needed. The corresponding PTM includes the following steps:

1. Establish a login as an administrator and retrieve/print the CRUD (Create, Retrieve, Update, and Delete) commands related to security parameters, such as: user-ID, password, the number of incorrect login attempts in succession to set an alarm, password aging interval, interval of inactivity before time-out occurs, user privilege, privilege associated with point of ingress, events to be recorded in security logs, and contents of security logs.
2. If any of these CRUD commands, except for three disallowed commands,[15] are missing (i.e., if the corresponding security parameters are hard-coded so that they cannot created, edited, retrieved, or deleted by an administrator), the TOE fails the test.
3. Establish a login as an administrator and attempt to execute the three disallowed commands, namely: (a) retrieve passwords in plaintext, (b) modify records in a security log, and (c) delete a security log. The TOE should deny all these transactions. Otherwise, the TOE fails the test.

[15] There are three CRUD commands that no user, including an administrator should be allowed to execute, namely: (1) retrieving passwords in plaintext, (2) modifying the records of a security log, (3) deleting a security log.

4. If the TOE passes Step 2, i.e., if the above-mentioned CRUD commands exist, check the user privileges assigned to the CRUD commands. If these privileges indicate that the CRUD commands can be executed by any user other than an administrator, the TOE fails the test.
5. To confirm the observations made in Step 4, establish a login as a user with a privilege lower than that of an administrator, and attempt to execute the CRUD commands on the security parameters listed in Step 1. The TOE should deny all the transactions. If not, the TOE fails the test.
6. Establish a login as an administrator. If the TOE has other points of ingress, establish simultaneous logins as users at the other points of ingress. Execute an appropriate command as the administrator to display the user-IDs that are concurrently logged on at the other ingresses. If the administrator does not have this capability, the TOE fails the test.
7. If the TOE passes Step 6, continue by executing appropriate commands as the administrator to display the transactions that are being executed by other users who are concurrently logged on. If the administrator does not have this capability, the TOE fails the test.

5.3.7 Packaging & Delivery

Proper Packaging & Delivery ensures secure installation, e.g., the software being delivered is the correct software and the security restrictions are all in place at the time of delivery. For example, default logins such as admin/admin should be deleted at the installation time. The corresponding PTM includes the following steps:

1. At the installation time, attempt to establish sessions at all the points of ingress (except the EAI) to ascertain that the appropriate login features have been activated. If the TOE allows a session without requiring a login with a user-ID and an authenticator, the TOE fails the test.
2. Establish a session at the EAI and attempt to restore the TOE from backup media (or the source code, if available). If the TOE cannot be restored, it fails the test.
3. At the installation time, establish a session as an administrator and customize the default user-ID and the default password. If the TOE denies this transaction, it fails the test.
4. At the installation time, perform the test to ensure that the software being installed is exactly as specified in the master copy. If there are no tools to perform this comparison, the TOE fails the test.
5. At the installation time, perform the test to ensure that all the software component modules are consistent with the software release. If there are no tools for this confirmation, the TOE fails the test.

5.3.8 Y2K Compliance

This feature deals with the integrity of the date-sensitive security parameters of the TOE when the time clock changes over a “sensitive date-transition.” Examples of sensitive date-transition are:

- From 9/8/99 to 9/9/99
- From 12/31/99 to 1/1/00
- From 2/28/00 to 2/29/00
- From 2/29/00 to 3/1/00
- From 12/31/00 to 1/1/01

Examples of date-sensitive security parameters are:

- A display at the login time that indicates the date and time of the last login
- Password aging
- Advance notice of imminent password expiration
- Password grace period (i.e., the old password may still be allowed a finite number of times beyond expiration)
- Password Updating (which requires a minimum waiting period)
- Duration of a channel lockout when password cracking is suspected
- The time-out feature
- Date stamps on resource creation, modification or deletion
- Entries in the security log carrying date and time stamps
- Functions set up for delayed action (e.g., a function set up in the afternoon that a report will be printed in the following morning)

The scope consists of testing the integrity of each date-sensitive parameter for each sensitive date-transition. At a generic level, the PTM consists of the following steps:

1. Establish a login as an administrator and set the clock at the beginning of a sensitive date-transition (e.g., 11:50 PM on 9/8/99).
2. Activate the security parameter to be tested. For example, to test the integrity of the password-aging feature, create a user-ID and a password. Assign a suitable aging interval (e.g., one day).
3. Advance the clock over the transition between 9/8/99 to 9/9/99, and test whether the TOE complies with the aging interval, i.e., the password should remain valid until 11:50 PM on 9/9/99, after which the password should expire.
4. Repeat the above generic test-template for each date-sensitive security parameter for each sensitive date-transition.

If the TOE fails any of these tests, it is not Y2K-compliant.

6. Conclusion

This document describes a methodology for testing the protection profile of a PBX switching system. The objective of these tests is to determine the level of security that a switching system can attain, assuming that the security-related features that are available in the system are properly activated. Thus the methodology boils down to determining the security features that are available in the system. Whether, in any given system, the available features have been activated or not is a question that is addressed in a security audit. By contrast, security testing is an effort to identify the features that the system offers.

The PBX is usually equipped with adjuncts such as a voice mail system and an automated attendant. It is necessary to secure all these components. With new and emerging technology, there is a tendency towards having a distributed architecture for the PBX, which may consist of numerous broadband switches and routers connected over a network. Such an architecture increases the number of possible ingresses into the system and hence the vulnerability of the system.

The vulnerability of the PBX can be grouped into two categories: (1) fraud committed over the traffic channels, and (2) breaking into the operations channels. Tests have been described to assess both types of security issues.

Since there is a wide range of PBXs and their adjuncts, the details of a test script are expected to be application-specific. The methodology described in this document is intended to provide a uniform template that can be used by a test-script writer to develop application-specific test scripts.